CLAIMS

1. A random number generation apparatus comprising:

random noise generation means for generating random noise by measuring physical noise;

random pulse wave generation means for generating a random pulse wave by waveshaping the random noise;

binary pulse sequence conversion means for sampling the random pulse wave at a clock of a constant period and converting it into a binary pulse sequence of a constant period, which has on/off of the sampled values as a pulse code; and

binary pulse sequence code smoothing means for reversing polarity of the binary pulse sequence at intervals of a constant period and smoothing appearance balance of 1/0 code in a specified unit of code length,

wherein a random number sequence of the smoothed binary pulse sequence code is generated.

2. The random number generation apparatus according to claim 1, wherein the random pulse wave is generated so that generation interval of the random noise is on/off time of pulse.

3. The random number generation apparatus according to claim 1, wherein random noise composed by using a plurality of the random noise generation means is inputted to the random pulse wave generation means and occurrence frequency

of on/off of the random pulse wave is increased.

4. The random number generation apparatus according to claim 1, wherein the random pulse wave generation means is constituted of pulse generation means, the output state of which changes for every input of the random noise as a trigger pulse.

5. The random number generation apparatus according to claim 1, wherein the binary pulse sequence code smoothing means is constituted of a 1/2 divider, which divides the clock frequency into half, and an XOR gate, which is inputted with output of the 1/2 divider and the binary pulse sequence.

6. The random number generation apparatus according to claim 1, wherein the binary pulse sequence code smoothing means is constituted of a 1/2 divider, which divides the clock frequency into half, and a logic circuit, which reverses the binary pulse sequence synchronizing with output of the 1/2 divider by turns to output the reversed binary pulse sequence.

ABSTRACT

In this invention, a random number generation apparatus inputs unperiodic random noise n generated by a noise source 1 to a waveform shaping circuit 2 to generate a random pulse wave P1. Next, the random number generation apparatus inputs the random pulse wave P1 and a clock c1 from an oscillator 3 to a sample-and-hold circuit 4 to generate a constant periodic binary pulse sequence P2. Subsequently, the binary pulse sequence P2 and a half divided clock c2, which is the clock c1 half divided by the divider 5, are inputted to a switching circuit 6, and the polarity of the binary pulse sequence P2 is reversed at intervals of one period to output a smoothed binary pulse sequence P3 in which appearance balance of 1/0 code is smoothed.